TUNNELING DEVICE

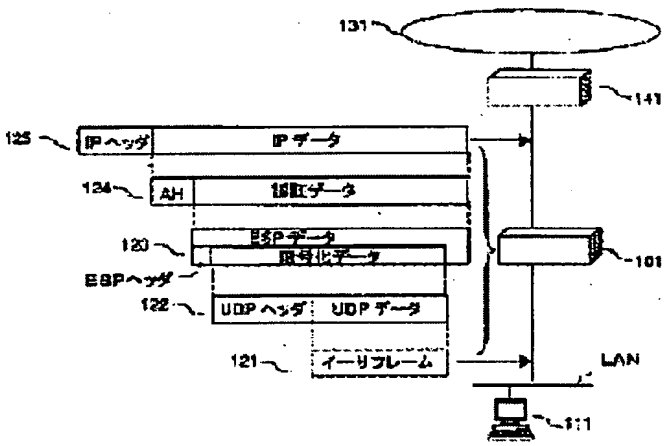
Patent number: JP2002271417
Publication date: 2002-09-20

Inventor: TERADA KIYONOBU; KAJIWARA MASAFUMI
Applicant: HITACHI CABLE; OSAKA MEDIA PORT CORP

Classification:
- international: H04L12/66; G06F13/00; G06F15/00; H04L12/46; H04L12/56
- european:
Application number: JP20010061941 20010306
Priority number(s): JP20010061941 20010306

Abstract of **JP2002271417**

PROBLEM TO BE SOLVED: To provide a tunneling device which is capable of operating LANs through an IP network as a common VPN. SOLUTION: An LAN-side port has a function of receiving the entire frame 121 of a data link layer flowing through a network, forming (encapsulated) an IP packet 125 that contains the received frame as data, and transmitting the IP packet 125 from the IP network-side port to a tunneling terminal station. An IP network-side port has a function of receiving the IP packet 125 addressed to it, taking out the frame 121 of the data link layer from the IP packet 125 when the IP packet 125 is the encapsulated frame of the data link layer, and transmitting the frame 121 from the LAN-side port.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－271417
（P2002－271417A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	12/66		Ｈ０４Ｌ 12/66	Ｂ	５Ｂ０８５
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ 13/00	３５１Ｂ	５Ｂ０８９
	15/00	３１０	15/00	３１０	５Ｋ０３０
Ｈ０４Ｌ	12/46	２００	Ｈ０４Ｌ 12/46	２００Ｘ	５Ｋ０３３
	12/56		12/56	Ｈ	

審査請求　未請求　請求項の数２　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－61941(P2001－61941)

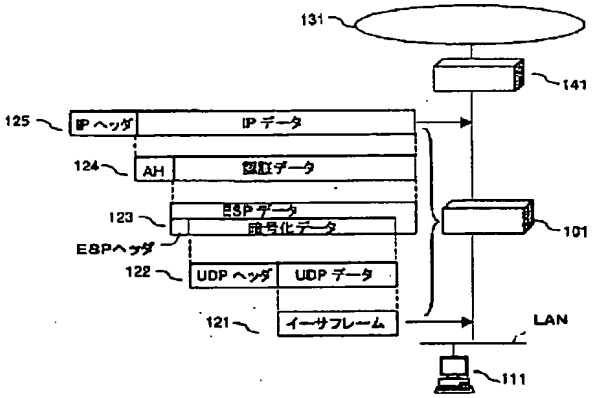
(22)出願日　平成13年３月６日(2001.3.6)

(71)出願人　000005120
日立電線株式会社
東京都千代田区大手町一丁目６番１号
(71)出願人　597056121
大阪メディアポート株式会社
大阪府大阪市北区中之島６丁目２番27号
(72)発明者　寺田　清伸
茨城県日立市日高町５丁目１番１号　日立電線株式会社オプトロシステム研究所内
(74)代理人　100068021
弁理士　絹谷　信雄

最終頁に続く

(54)【発明の名称】　トンネリング装置

(57)【要約】
【課題】　ＩＰ網を介したＬＡＮ同士を共通のＶＰＮとして運用可能とするトンネリング装置を提供する。
【解決手段】　ＬＡＮ側ポートでは、ネットワークを流れるデータリンク層のフレーム１２１全てを受信し、その受信したフレームをデータとするＩＰパケット１２５を作成（カプセル化）し、そのパケットをＩＰ網側ポートからトンネリングの終端局宛てに送信する機能を備え、ＩＰ網側ポートでは、自局宛てに送られてきたＩＰパケット１２５を受信し、そのＩＰパケット１２５がデータリンク層のフレームをカプセル化したものである場合には、そのＩＰパケット１２５からデータリンク層のフレーム１２１を取り出し、そのフレーム１２１をＬＡＮ側ポートから送信する。



1

【特許請求の範囲】

【請求項１】　ＯＳＩ参照モデルのデータリンク層のフレームを送受信することができるＬＡＮ側ポートとＯＳＩ参照モデルのネットワーク層のフレーム（パケット）を送受信することができるＩＰ網側ポートとを備え、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のＩＰアドレスを登録するバッファ部を備え、前記ＬＡＮ側ポートでは、ネットワークを流れるデータリンク層のフレーム全てを受信し、その受信したフレームをデータとするＩＰパケットを作成（カプセル化）し、そのパケットをＩＰ網側ポートからトンネリングの終端局宛てに送信する機能を備え、前記ＩＰ網側ポートでは、自局宛てに送られてきたＩＰパケットを受信し、そのＩＰパケットがデータリンク層のフレームをカプセル化したものである場合には、そのＩＰパケットからデータリンク層のフレームを取り出し、そのフレームをＬＡＮ側ポートから送信する機能を備えたことを特徴とするトンネリング装置。

【請求項２】　前記ＬＡＮ側ポートにおいて受信したデータリンク層フレームをカプセル化する際に、データの内容を暗号化し、その暗号化したデータに暗号化方式などを設定した暗号化ヘッダを付加し、さらに送信者の正当性を証明する認証ヘッダを付加する機能を備え、前記ＩＰ網側ポートにおいて受信したＩＰパケットからデータリンク層のフレームを取り出す際に、そのＩＰパケットに認証ヘッダが含まれている場合にはその認証ヘッダによりＩＰパケット送信者の正当性やデータ改竄の有無を検証し、さらに前記ＩＰパケットに暗号化ヘッダが含まれている場合には暗号化されているデータを復号化する機能を備えたことを特徴とする請求項１記載のトンネリング装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、広域の各地に点在する事業所や大学等のローカルエリアネットワークを専用線に比べて低コストなＩＰ網を使って接続し、仮想的なプライベートネットワークを構成するＶＰＮ技術に係り、特に、企業や大学、ＩＳＰ等に設置して使用するＶＰＮ装置のためのトンネリング装置に関するものである。

【０００２】

【従来の技術】端末が互いに遠隔地に存在するネットワークを安全に接続するためのＶＰＮ方式としてＲＦＣ２４０１等で規定されるＩＰｓｅｃを使用したもの、ＲＦＣ２６６１で規定されるＬ２ＴＰを使用したもの、ＲＦＣ２５４７で規定されるＭＰＬＳを使用したものの３つの方式が一般的に知られている。

【０００３】まず、図４を用いてＩＰｓｅｃを使用した方式について述べる。ＬＡＮ４２１，４２２をＩＰ網４３１を介して仮想的なプライベートネットワークとして

2

安全に接続するため、ＩＰｓｅｃ機能を搭載したルータ４４１，４４２を使って接続する。端末４１１～４１２と端末４１３～４１４との間で送受信されるパケットは、ルータ４４１，４４２によってＩＰｓｅｃの暗号化及び認証が行われ、インターネット上では図１４のＡＨヘッダが付加された状態、または図１５のＥＳＰペイロードフォーマットによりカプセル化された状態、またはその両方の状態でパケットが転送される。これにより、ＬＡＮ４２１，４２２間の通信内容がネットワーク上の第三者による盗聴やパケットの改竄から保護され、各端末が安全に通信を行うことができる。

【０００４】次に、図５を用いてＬ２ＴＰを使用した方式について述べる。この方式では、ＶＰＮ接続を行う端末は、まず電話回線５２３を使用してＬＡＣ５７１にＰＰＰで接続する。ＬＡＣ５７１は、このＰＰＰフレームに図１６に示すＬ２ＴＰヘッダを付加してＬ２ＴＰフレームとした後、このＬ２ＴＰフレームをＩＰ網５３１を経由してルータ５４２へパケットとして転送する。ルータ５４２はＬＮＳと呼ばれ、このＬ２ＴＰフレームをＬＡＮ５２２のフレームフォーマットに変換し、ＬＡＮ５２２上の端末に転送する。また、電話回線５２３を使用しない場合、上記ＬＡＣ機能を備えた専用ソフトを搭載した端末５１２（ＬＡＣクライアント）は、上記ＬＡＣ５７１と同様にＰＰＰフレームにＬ２ＴＰヘッダを付加し、そのＬ２ＴＰフレームをＬＡＮ５２２に転送し、ＬＡＮ５２２上の端末と通信を行う。これにより、ＩＰ網上でＬＡＣまたはＬＡＣクライアントからＬＮＳまでに仮想的なポイントトゥポイントコネクションが張られ、ＩＰ網を介して端末５１１，５１２をプライベートネットワークであるＬＡＮ５２２に安全に接続することができる。

【０００５】次に、図６を用いてＭＰＬＳを使用した方式について述べる。ＬＡＮとＩＰ網とを接続するルータ６４１，６４２はＬＥ(Label edge)ルータと呼ばれ、図１７に示すシムヘッダを付けてフレームを転送する機能を持つ。また、ＩＰ網内はシムヘッダ内のラベルに従ってパケットを交換する機能を持つＬＳＲ(Label Switch router) ６４３～６４５で接続する。端末６１１から端末６１３に送信されたフレームは、ＬＥルータ６４１によってシムヘッダが付加され、パケットとしてＩＰ網に送信された後、シムヘッダ内のラベルに従ってＬＳＲ６４３～６４５によって転送される。そのパケットがＬＥルータ６４２まで到達すると、ＬＥルータ６４２はこのシムヘッダを取り外し、フレームを端末６１３に転送する。ＬＳＲ間で行われるパケット転送は、ネットワークアドレスではなくＬＥ６４１で付けられたラベルのみを参照して行われるため、他のネットワークから送信されたパケットが転送されることがなく、ＬＡＮ６２１とＬＡＮ６２２との間の通信が保護される。

【０００６】ここで、本明細書に使用される略語の日本

語表記又は簡単な説明を列記しておく。

【０００７】ＯＳＩ(Open Systems Interconnection)参照モデル：国際標準化機構が定める開放型システム間相互接続参照モデル。２層はデータリンク層、３層はネットワーク層、４層はトランスポート層と呼ばれる。

【０００８】ＩＰ(Internet Protocol) ：インターネットプロトコル（ネットワーク層）

ＴＣＰ／ＩＰ(Transport Control Protocol/Internet Protocol)：インターネットの標準プロトコル群

UDP(User Datagram Protocol)：コネクションレス型のトランスポート層プロトコル

ＴＣＰ(Transmission Control Protocol) ：コネクション型のトランスポート層プロトコル

ＶＰＮ(Virtual Private Network) ：仮想私設網

ＩＳＰ(Internet Service Provider) ：インターネットサービスプロバイダ

ＲＦＣ(Request for Comments)：インターネットアーキテクチャ委員会による標準勧告文書、２４０１、２６６１、２５４７などはその文書の番号

ＩＰｓｅｃ(IP security) ：インターネットプロトコルセキュリティ

ＥＳＰ：ＩＰｓｅｃにより作成した暗号化データ、ヘッダを示す名称

Ｌ２ＴＰ(Layer Two Tunneling Protocol)：レイヤ２トンネリングプロトコルＭＰＬＳ(Multi Protocol Label Switching)：マルチプロトコルラベルスイッチング

ＬＡＣ(L2TP Access Concentrator)：Ｌ２ＴＰアクセスコントローラ

ＰＰＰ(Point to Point Protocol) ：公衆回線でＩＰ接続するためのプロトコル

ＬＮＳ(LT2P Network Server) ：Ｌ２ＴＰネットワークサーバ

ＩＥＥＥ(Institute of Electrical and Electronics Engineers) ：アメリカ電気・電子技術者協会

ＩＰｖ６(IP version 6)：アドレス長を長くしたＩＰ

ＮｅｔＢＩＯＳ(Network Basic Input/Output System) ：ネットワーク基本入力システム

ＩＰＸ(Internetwork Packet Exchange)：ノベル社のネットワーク層プロトコル

ＡｐｐｌｅＴａｌｋ：アップル社のネットワークＯＳ

以上に列記しないものも含め本明細書に使用される略語、用語は、いずれも公知の文献に記載されているものであり、本明細書では詳細な説明は省略する。

【０００９】

【発明が解決しようとする課題】従来技術において、ＩＰｓｅｃを使用した方式では、ネットワーク層においてＩＰパケットの暗号化とカプセル化とを行うため、通信可能なプロトコルがＩＰに限定されてしまう。

【００１０】また、Ｌ２ＴＰを使用した方式では、クライアントがＰＰＰ接続しているか、または専用ソフトを使用しなければならず、特定のクライアントしかＶＰＮを利用することができない。

【００１１】また、ＭＰＬＳを使用した方式では、ＭＰＬＳに対応したルータで構成されたネットワーク内でしか通信できないという問題がある。

【００１２】そこで、本発明の目的は、上記課題を解決し、ＩＰ網を介したＬＡＮ同士を共通のＶＰＮとして運用可能とするトンネリング装置を提供することにある。

【００１３】

【課題を解決するための手段】上記目的を達成するために本発明は、ＯＳＩ参照モデルのデータリンク層のフレームを送受信することができるＬＡＮ側ポートとＯＳＩ参照モデルのネットワーク層のフレーム（パケット）を送受信することができるＩＰ網側ポートとを備え、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のＩＰアドレスを登録するバッファ部を備え、前記ＬＡＮ側ポートでは、ネットワークを流れるデータリンク層のフレーム全てを受信し、その受信したフレームをデータとするＩＰパケットを作成（カプセル化）し、そのパケットをＩＰ網側ポートからトンネリングの終端局宛てに送信する機能を備え、前記ＩＰ網側ポートでは、自局宛てに送られてきたＩＰパケットを受信し、そのＩＰパケットがデータリンク層のフレームをカプセル化したものである場合には、そのＩＰパケットからデータリンク層のフレームを取り出し、そのフレームをＬＡＮ側ポートから送信する機能を備えたものである。

【００１４】前記ＬＡＮ側ポートにおいて受信したデータリンク層フレームをカプセル化する際に、データの内容を暗号化し、その暗号化したデータに暗号化方式などを設定した暗号化ヘッダを付加し、さらに送信者の正当性を証明する認証ヘッダを付加する機能を備え、前記ＩＰ網側ポートにおいて受信したＩＰパケットからデータリンク層のフレームを取り出す際に、そのＩＰパケットに認証ヘッダが含まれている場合にはその認証ヘッダによりＩＰパケット送信者の正当性やデータ改竄の有無を検証し、さらに前記ＩＰパケットに暗号化ヘッダが含まれている場合には暗号化されているデータを復号化する機能を備えてもよい。

【００１５】

【発明の実施の形態】以下、本発明の一実施形態を添付図面に基づいて詳述する。

【００１６】図１に示されるように、本発明に係るトンネリング装置１０１は、ＬＡＮ側の伝送路に接続されるＬＡＮ側ポートとＩＰ網１３１側の伝送路に接続されるＩＰ網側ポートとを備え、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のＩＰアドレスを登録するバッファ部を内部に備えている。

【００１７】このトンネリング装置１０１は、ＬＡＮから受信したデータリンク層のフレーム（ここではイーサ

5

ネット（登録商標）フレーム；イーサフレームともいう）１２１をＵＤＰデータとし、このＵＤＰデータにＵＤＰヘッダを付加してフレーム１２２を作成するＵＤＰフレーム作成手段と、このＵＤＰヘッダを含むフレーム１２２全体を所定の暗号化方式（ここではＩＰｓｅｃに基づく暗号化方式）で暗号化し、この暗号化データにＥＳＰヘッダ及びトレーラを付加してフレーム（ＥＳＰデータ）１２３を作成する暗号化手段と、このフレーム１２３にこのフレーム１２３を認証データとする認証ヘッダ（ここではＡＨヘッダ）を付加してフレーム１２４を作成する認証情報付加手段と、このフレーム１２４をＩＰデータとし、このＩＰデータにバッファ部に登録されているＩＰアドレスを用いたＩＰヘッダを付加してネットワーク層のフレーム（ＩＰパケット）１２５を作成（カプセル化）するカプセル化手段とを備える。

【００１８】また、このトンネリング装置１０１は、ＩＰ網１３１から受信したネットワーク層のフレーム（ＩＰパケット）が上記カプセル化によるＩＰパケット１２５であることを認識するカプセル化認識手段と、そのＩＰデータであるフレーム１２４に含まれている認証ヘッダを認識して認証データの認証を行う認証手段と、その認証データ（フレーム１２３）に含まれている暗号化ヘッダを認識して暗号化データを復号化してＵＤＰフレーム１２２を復元する復号化手段と、そのＵＤＰフレーム１２２からデータリンク層のフレーム１２１を取り出すフレーム取出手段とを備える。

【００１９】１１１はＬＡＮに接続された端末、１４１はＩＰ網１３１との中継を行うルータである。図１には、トンネリング装置１０１が１つしか示されていないが、ＩＰ網１３１に複数のトンネリング装置１０１が繋がることにより、トンネリング装置相互間の送受信が実現できる。その例を図２により説明する。

【００２０】図２において、ＬＡＮ２２１は事業所Ａのイーサネット、ＬＡＮ２２２は事業所Ｂのイーサネット、ＩＰ網２３１はインターネット、２０１、２０２は、本発明に係るトンネリング装置、２４１、２４２はルータである。トンネリング装置２０１、２０２のＩＰ網側ポート２５１、２５４はルータ２４１、２４２にそれぞれ接続され、ＩＰ網側ポート２５１、２５４のデータリンク層の通信媒体はイーサネットである。ＬＡＮ側ポート２５２、２５３は、ＬＡＮ２２１、２２２にそれぞれ接続されている。ＬＡＮ２２１、２２２の端末２１１～２１４にはＴＣＰ／ＩＰプロトコルが実装されている。

【００２１】各端末２１１～２１４、各トンネリング装置２０１、２０２及び各ルータ２４１、２４２のインタフェースのＩＰアドレス及びＭＡＣアドレスは図７のようになっているものとする。ただし、図７において、「インタフェース」と書かれている欄は、図２における各部材の符号を示している。従って、例えば、端末２１１のＭＡＣアドレスは、“００：００：００：００：００：０１”、ＩＰアドレスは、“１９２．０．０．１／２４”である。

6

【００２２】トンネリング装置２０１、２０２のＵＤＰポート番号は、“１７０１”に設定されているものとする。

【００２３】トンネリング装置２０１、２０２のソフトウェア構成は、図８のようになっているものとする。即ち、トンネリング装置２０１、２０２は、ソフトウェアとして少なくとも、ＬＡＮ側ポート及びＩＰ網側ポートにおけるイーサネットに係る処理を行うイーサネットドライバと、ＴＣＰ／ＩＰ及びＩＰｓｅｃソフトウェアと、本発明に係るトンネリングソフトウェアとを備える。図１で説明した各手段は、これらのソフトウェアで実現されている。

【００２４】トンネリング装置２０１、２０２のハードウェア構成は、図１８のようになっているものとする。即ち、トンネリング装置２０１、２０２は、ＯＳＩ参照モデルのデータリンク層のフレームを送受信することができるＬＡＮ側ポート１８０１と、ＯＳＩ参照モデルのネットワーク層のフレームを送受信することができるＩＰ網側ポート１８０２と、自局をトンネリングの始点としたときのトンネリングの終点となる終端局のＩＰアドレスを登録するバッファ部を含む主記憶装置１８０３と、図８のソフトウェアを実行するＣＰＵ１８０４と、補助記憶装置１８０５とを有する。

【００２５】図２のように場所などが異なる２つのＬＡＮ２２１、２２２をＶＰＮ接続し、端末２１１と端末２１３との間で安全に通信する本発明の手順を以下に述べる。なお、本実施形態では、ＶＰＮのセキュリティ機能を提供する手段として、通信路上のデータの暗号化及び認証を行うＩＰｓｅｃを利用した。

【００２６】まず、端末２１１から端末２１３へ宛ててＬＡＮ２２１へフレームが送信されたものとする。

【００２７】トンネリング装置２０１は、ＬＡＮ２２１を流れるフレームを宛先に関わらず全てプロミスキャス（無差別）に受信し、受信したフレーム（図１のフレーム１２１）に宛先ポート番号を“１７０１”に設定したＵＤＰヘッダを付加する（フレーム１２２）。ＵＤＰヘッダは、図１２に示すフォーマットで作成される。図１２において、１２０１が宛先ポート番号“１７０１”を格納するフィールドである。

【００２８】次に、トンネリング装置２０１は、ＵＤＰフレーム１２２全体を暗号化し、ＥＳＰヘッダ及びトレーラを付加してＥＳＰデータ（フレーム１２３）を作成する。ＥＳＰペイロードは、図１５に示すフォーマットで作成される。

【００２９】次に、トンネリング装置２０１は、パケットの正当性を証明するＡＨヘッダを付加する（フレーム１２４）。ＡＨヘッダは、図１４に示すフォーマットで

作成される。

【００３０】次に、トンネリング装置２０１は、自局（トンネリング装置２０１）をトンネリングの始点としたときのトンネリングの終点となる終端局（ここではトンネリング装置２０２）のＩＰアドレスをバッファ部の内容（図７）から判定し、ＩＰ網側ポート２５４のＩＰアドレス“２０．０．０．２／２４”を用いてトンネリング装置２０２を宛先とするＩＰヘッダを作成し、このＩＰヘッダをフレーム１２４に付加することにより、ＩＰパケット（フレーム１２５）を作成する。ＩＰヘッダは、図１１に示すフォーマットで作成される。図１１において１１０１が宛先ＩＰアドレスを格納するフィールドである。トンネリング装置２０１は、このフレーム１２５をＩＰ網側ポート２５１からルータ２４１のポート２６１へ送信する。

【００３１】なお、ＩＰ網側ポート２５１に接続するデータリンク層の通信方式（通信媒体）はイーサネットであるため、ＩＰ網側ポート２５１から実際に送信されるフレームの形式は、作成されたＩＰパケット（フレーム１２５）をデータとして、図９のＩＥＥＥ８０２．２／８０２．３カプセル化又は図１０のイーサネットカプセル化が行われた形式となる。図９、１０において、９０１、１００１がＩＰパケットをデータとして格納するフィールドである。

【００３２】ルータ２４１のポート２６２よりＩＰ網２３-１に送信されたＩＰパケットは、ルータ２４２のポート２６３へ到着し、ポート２６４よりトンネリング装置２０２のＩＰ網側ポート２５４に送信される。

【００３３】トンネリング装置２０２は、ＩＰ網から自局のＵＤＰポート“１７０１”宛てのＩＰパケット（フレーム１２５）（ＩＰヘッダに格納されている宛先ＩＰアドレスが“２０．０．０．２／２４”）を受信した場合、フレーム１２４のＡＨヘッダによりパケットの正当性を確認し、フレーム１２３のＥＳＰデータの復号化を行い、フレーム１２２のＵＤＰヘッダを取り除いて元のイーサネットフレーム（フレーム１２１）を取り出し、そのフレームをＬＡＮ側ポート２５３からＬＡＮ２２２に送信する。

【００３４】このフレームは、端末２１３に到着する。このようにして、端末２１１から送信されたフレームが端末２１３に受信される。

【００３５】端末２１３から端末２１１へ宛ててＬＡＮ２２２へフレームが送信された場合についても、トンネリング装置２０２がトンネリング装置２０１と同様に、ＬＡＮ側ポート２５３で受信したフレームを前述と同様の処理（ＩＰｓｅｃ処理、ヘッダ付加処理）によりカプセル化した後、トンネリング装置２０１のＵＤＰポート（番号１７０１）に宛ててＩＰ網側へ送信する。トンネリング装置２０１は、ＩＰ網側から自局のＵＤＰポート（番号１７０１）で受信したＩＰパケットから前述と同様の処理（ＩＰｓｅｃ処理、ヘッダ除去処理）によりイーサネットフレームを取り出した後、そのフレームをＬＡＮ側ポート２５２からＬＡＮ２２１に送信する。こうして、端末２１３から送信されたフレームが端末２１１に受信される。

【００３６】なお、本実施形態では、ＵＤＰポート番号として１７０１番を使用しているが、他の番号でも構わない。

【００３７】また、本実施形態では、データリンク層のフレームにＵＤＰヘッダとＩＰヘッダとを付加したが、ＴＣＰヘッダとＩＰヘッダとを付加してもよく、或いは独自のトランスポート層ヘッダとＩＰヘッダとを付加してもよく、或いはＩＰヘッダのみをを付加してもよい。ＴＣＰヘッダのフォーマットは、図１３に示すとおりである。

【００３８】ここで、端末２１１が端末２１３宛てのイーサネットフレームを送信した場合の具体的な例として、端末２１１が端末２１３のＭＡＣアドレスを解決するためにＡＲＰ要求フレームをＬＡＮ２２１内の全端末にブロードキャスト送信した場合について説明する。端末２１１が送信したＡＲＰ要求フレームは、トンネリング装置２０１によってカプセル化されトンネリング装置２０２へ転送される。トンネリング装置２０２は、取り出したＡＲＰ要求フレームをＬＡＮ２２２内の全端末にブロードキャスト送信する。端末２１３は、このＡＲＰ要求フレームを受信すると、ＡＲＰ応答フレームを端末２１１宛てにユニキャスト送信する。このＡＲＰ応答フレームは、トンネリング装置２０２によってカプセル化されトンネリング装置２０１へ転送される。トンネリング装置２０１は、取り出したＡＲＰ応答フレームをＬＡＮ２２１にユニキャスト送信する。端末２１１は、このＡＲＰ応答フレームを受信することになる。

【００３９】本発明によれば、ＩＰｓｅｃの暗号化によりインタフェース上のデータは保護され、認証によりＬＡＮ２２１、２２２以外のネットワークからの接続を拒否できるので、ＬＡＮ２２１とＬＡＮ２２２との間でＶＰＮを構築することが可能となる。また、このときＬＡＮ２２１、２２２は、ハブやスイッチで接続されている同じＬＡＮセグメントと等価である。

【００４０】本実施形態では、場所などが異なる２つのイーサネットを同じＩＰサブネットとしてＶＰＮを構築したが、イーサネットではない他のデータリンク層の通信方式であっても、また、ＩＰ以外のネットワーク層プロトコルを使用した場合であっても、本発明によりＶＰＮを構築することができる。

【００４１】また、図３に示すように、端末３１１～３１２のデフォルトゲートウェイをルータ３４１に設定し、ハブやスイッチを使用してトンネリング装置３０１を介さずにイーサネットフレームを直接ルータ３４１に送信することにより、ＬＡＮ３２１上の端末３１１～３

１２がトンネリング装置を介していないインターネット上の端末（例えば、３１３～３１４）と通信を行うことが可能である。このように、本発明のトンネリング装置を用いたネットワークは、相手側のネットワークに本発明のトンネリング装置が存在しない場合でも、相手側のネットワークとの通信が可能である。

【００４２】

【発明の効果】本発明は次の如き優れた効果を発揮する。

【００４３】（１）請求項１の発明により、トンネリング装置で接続される２つのＬＡＮは、間にＩＰ網を介しているにも関わらず、ハブやスイッチで接続されたのと同様に、同一のネットワークとして振る舞うことができる。

【００４４】（２）請求項１の発明は、ＩＰｓｅｃを使用した方式とは異なり、２つのＬＡＮをネットワーク層ではなくデータリンク層で接続するため、２つのＬＡＮ間に使用するネットワーク層のプロトコルは、ＩＰプロトコルに限定されず、ＩＰｖ６やＮｅｔＢＩＯＳ、ＩＰＸ、ＡｐｐｌｅＴａｌｋ等のあらゆるプロトコルの通信が可能となる。

【００４５】（３）請求項２の発明のように、ＩＰｓｅｃ等のセキュリティ機能を組み込むことによって２つのＬＡＮ間の通信内容をネットワーク上の第三者による盗聴やパケットの改竄から防ぎ、パブリックなＩＰ網を介していながら安全に接続することが可能である。

【００４６】（４）請求項２の発明は、Ｌ２ＴＰを使用した方式とは異なり、ＰＰＰ接続や専用ソフトも必要ない。また、ＭＰＬＳを使用した方式のようにＩＰ網上のルータをＭＰＬＳ専用のルータに置き換えたり設定変更する必要もない。なお、セキュリティの強度に関してはＩＰｓｅｃを使用した方式と同等になる。

【図面の簡単な説明】

【図１】本発明の一実施形態を示すトンネリング装置の構成図である。

【図２】本発明のトンネリング装置を用いたネットワークの構成図である。

【図３】本発明のトンネリング装置を用いたネットワークの構成図である。

【図４】ＩＰｓｅｃ方式によるＶＰＮの構成図である。

【図５】Ｌ２ＴＰ方式によるＶＰＮの構成図である。

【図６】ＭＰＬＳ方式によるＶＰＮの構成図である。

【図７】図２のネットワークにおける各機器のアドレス割り当て図である。

【図８】図１のトンネリング装置のソフトウェア構成図である。

【図９】本発明によるＩＰパケットをＩＥＥＥ８０２．２／８０２．３カプセル化したフレームの構成図である。

【図１０】本発明によるＩＰパケットをイーサネットカプセル化したフレームの構成図である。

【図１１】ＩＰヘッダの構成図である。

【図１２】ＵＤＰヘッダの構成図である。

【図１３】ＴＣＰヘッダの構成図である。

【図１４】ＩＰｓｅｃで用いるＡＨヘッダの構成図である。

【図１５】ＩＰｓｅｃで用いるＥＳＰペイロードの構成図である。

【図１６】Ｌ２ＴＰヘッダの構成図である。

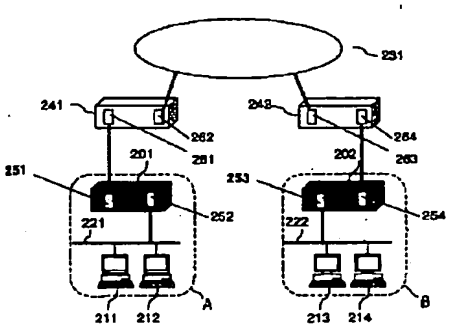
【図１７】ＭＰＬＳで用いるシムヘッダの構成図である。

【図１８】図１のトンネリング装置のハードウェア構成図である。

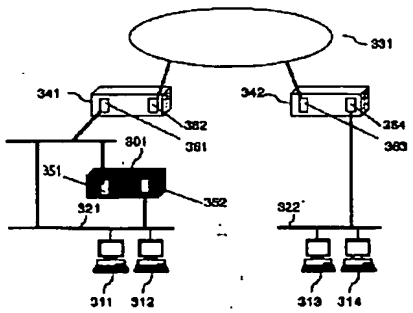
【符号の説明】

１０１、２１０、２０２、３０１　トンネリング装置
１３１、２３１、３３１　ＩＰ網
２２１、２２２、３２１、３２２　ＬＡＮ
２５１、２５４、３５１、１８０２　ＩＰ網側ポート
２５２、２５３、３５２、１８０１　ＬＡＮ側ポート
１８０３　バッファ部

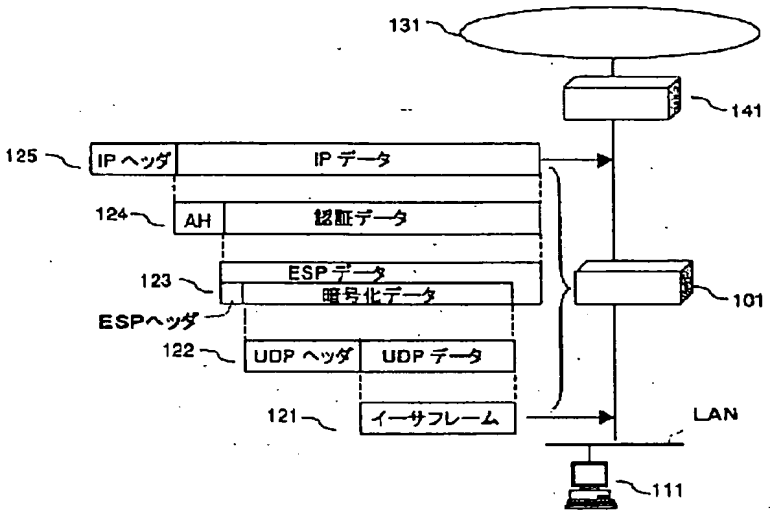
【図２】



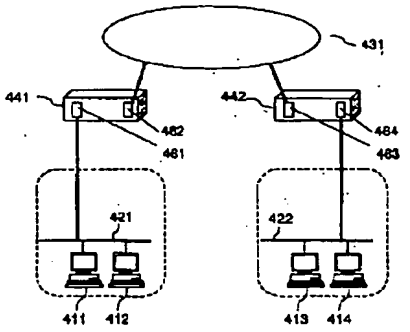
【図３】



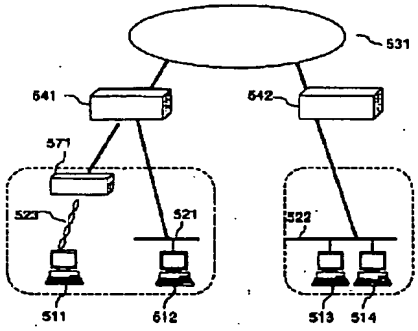
【図１】



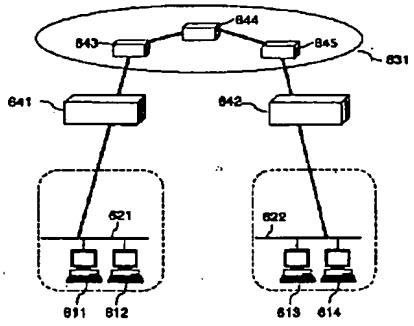
【図４】



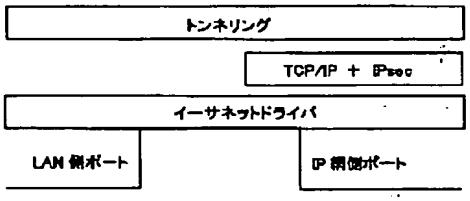
【図５】



【図６】



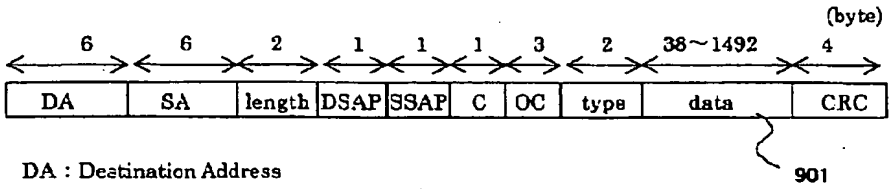
【図８】



【図７】

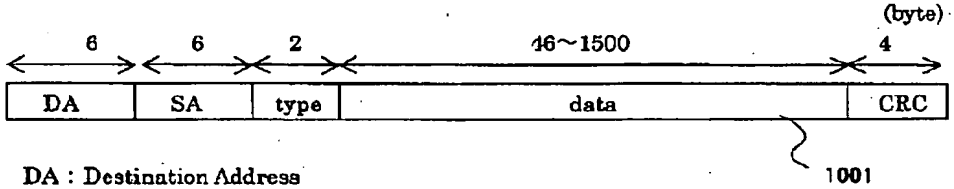
インタフェース	MAC アドレス	IP アドレス
211	00:00:00:00:00:01	192.0.0.1/24
212	00:00:00:00:00:02	192.0.0.2/24
213	00:00:00:00:00:03	192.0.0.3/24
214	00:00:00:00:00:04	192.0.0.4/24
251	00:00:00:00:00:05	10.0.0.1/24
252	00:00:00:00:00:06	なし
253	00:00:00:00:00:07	なし
254	00:00:00:00:00:08	20.0.0.2/24
261	00:00:00:00:00:09	10.0.0.3/24
262	00:00:00:00:00:0a	1.0.0.1/24
263	00:00:00:00:00:0b	2.0.0.1/24
264	00:00:00:00:00:0c	20.0.0.2/24

【図９】



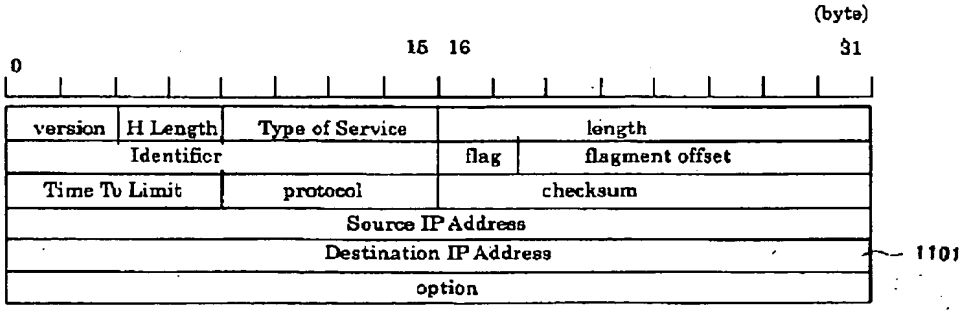
DA : Destination Address
SA : Source Address
DSAP : Destinatin Service Access Point
SSAP : Source Service Access Point
C : Control
OC : Original Code
CRC : Cyclic Redundancy Check

【図１０】

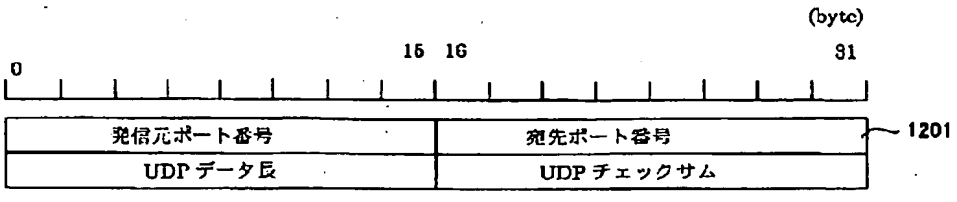


DA : Destination Address
SA : Source Address
CRC : Cyclic Redundancy Check

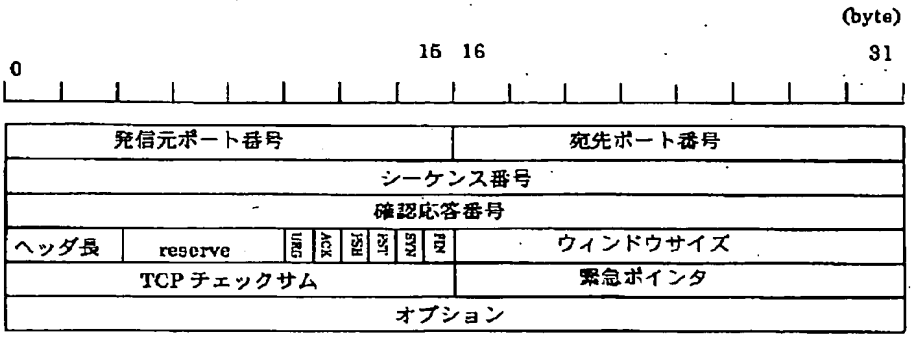
【図１１】



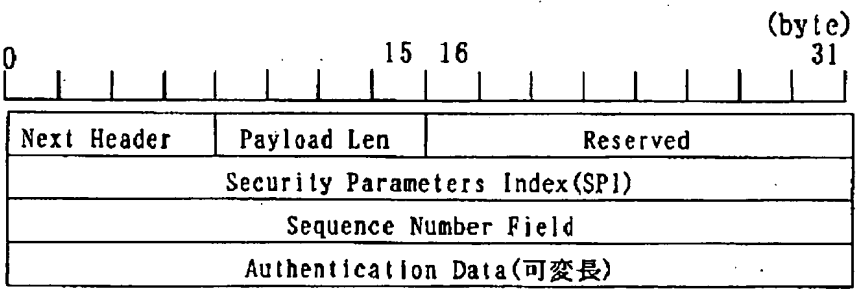
【図１２】



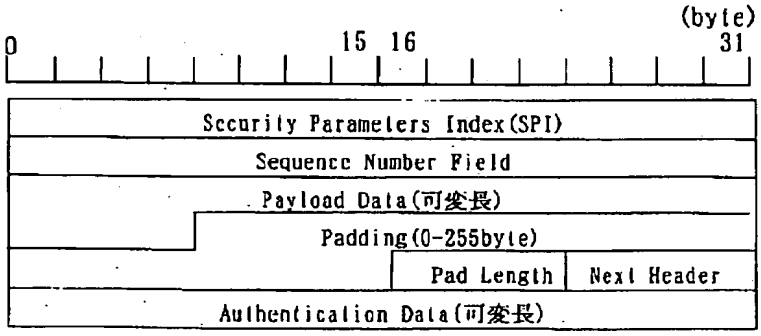
【図１３】



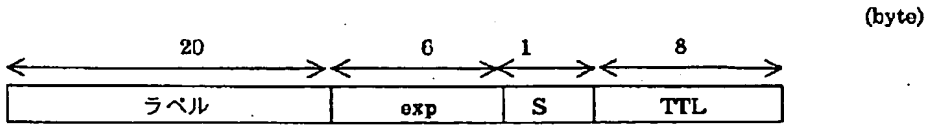
【図１４】



【図１５】

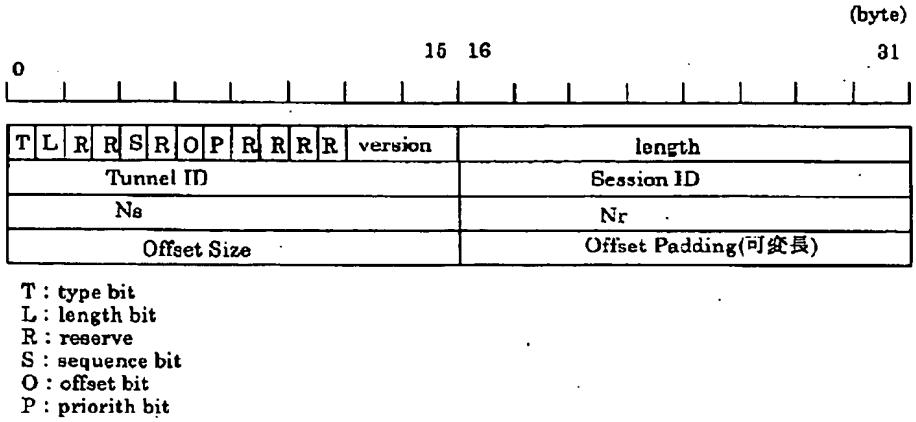


【図１７】



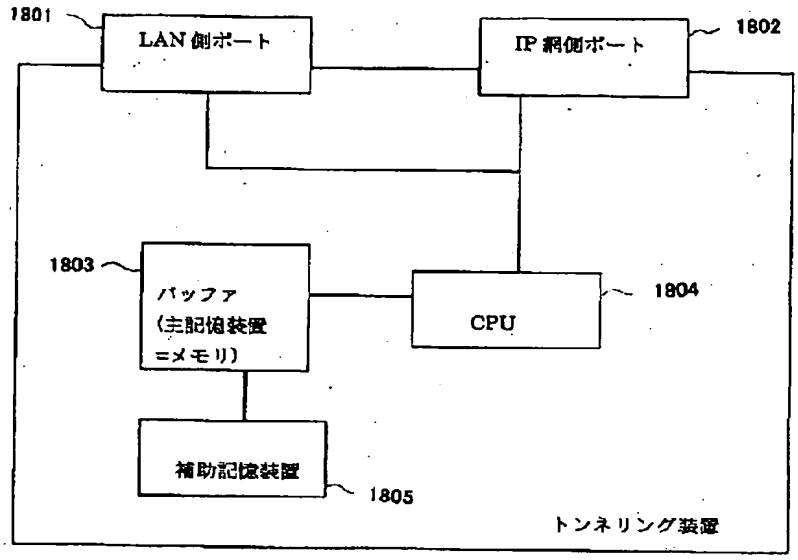
exp：実験用
S：ラベルスタックの最後を指定
TTL：Time To Live

【図１６】



T : type bit
L : length bit
R : reserve
S : sequence bit
O : offset bit
P : priorith bit

【図１８】



フロントページの続き

(72)発明者 梶原 将文
大阪府大阪市北区中之島６丁目２番40号
大阪メディアポート株式会社内

Ｆターム(参考) 5B085 AE00 AE29 BA07 BG07
5B089 GA04 GA31 HA06 HA10 HB19
JB24 KA04 KA09 KB04 KB06
KC28 KC47 KD01 KE02 KE03
KF05 KH04 KH30
5K030 GA15 HA08 HB18 HC01 HD03
HD06 HD09 JA05 KA13 LA07
LD19 LE11
5K033 AA09 BA02 CA08 CB08 CB11
CC01 CC04 DA06 DB10 DB19